AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of

INFORMATION ASSOCIATED WITH [redacted] THAT IS STORED AT PREMISES CONTROLLED BY GODADDY.COM, LLC

Case No. 4:17 MJ 5191 NAB

APPLICATION FOR A SEARCH WARRANT

I, Wendy J. Rowan, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

Informaton associated with [redacted] that is stored at premises controlled by GoDaddy.com, LLC

located in the _____ District of Arizona, there is now concealed

See Attachment A.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Section 287	False, fictitious or fraudulent claims
18 U.S.C. Section 1001	False Statements
18 U.S.C. Section 371	Conspiracy to commit offense or to defraud the United States
18 U.S.C. Section 1341	Mail Fraud

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Wendy Jo Rowan
Applicant's signature

Special Agent Wendy J. Rowan
General Services Administration/OIG
Printed name and title

Sworn to before me and signed in my presence.

Date: 8/3/17

Judge's signature

City and state: St. Louis, MO

Honorable Nannette A. Baker, U.S. Magistrate Judge
Printed name and title

AUSA: STEVEN A. MUCHNICK

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF	)	
INFORMATION ASSOCIATED WITH	)	Case No. 4:17 MJ 5191 NAB
[redacted] THAT IS STORED AT	)	
PREMISES CONTROLLED BY	)	**Filed Under Seal**
GODADDY.COM, LLC	)	

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A FOR SEARCH WARRANT

I, Wendy J. Rowan, being first duly sworn, hereby depose and state the following:

INTRODUCTION

A. Background

1. I, Wendy J. Rowan, am a Special Agent with General Services Administration, Office of Inspector General (GSA-OIG), and have been so employed since 2001. As such, I am a federal law enforcement officer of the United States empowered by federal law to conduct investigations of and make arrests for offenses enumerated in Title 18, United States Code (USC).

2. I hold a Bachelor of Science degree from Minnesota State University, Mankato, Minnesota. Throughout my career as a special agent, I have received training and conducted investigations regarding violations of federal criminal law, including Title 18, United States Code.

3. During my career I have investigated violations of federal criminal law in white collar fraud, property crimes, general crimes and computer-related crimes. I have gained experience through training, seminars, classes, and everyday work related to conducting these types of investigations. Based on my experiences, I am familiar with the techniques used by persons who are engaged in fraudulent and other related criminal activity.

4. Training included the investigation of financial crimes, such as tax evasion, filing of false tax returns, bribery, kickbacks, racketeering, money laundering, violations of the Bank Secrecy Act and conspiracy. I also received instruction on probable cause as it relates to search and seizure warrants, and methods and practices of executing such warrants. I have over fifteen years of experience and have assisted in the execution of search warrants of personal residences and businesses for personal and business records relevant to ongoing criminal property crimes and financial investigations. Through my education, training and experience as a Special Agent, I have become familiar with the manner in which individuals and entities prepare and maintain both personal and business records.

5. I make this affidavit in support of an application for a search warrant under Title 18, U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require GoDaddy.com, LLC to disclose to the government copies of the information (including the content of communications) further described in Attachment A. Upon receipt of that information, government-authorized persons will review that information to locate the items described in Section II of Attachment A.

6. The information contained within this affidavit is either personally known by me or was provided to me by Confidential Informant [redacted] (CI). I have also discussed with my colleagues the use of computers to create, store, and use electronic data over Internet-based applications, and how criminals, and their supporters or conspirators, use computers and the Internet to facilitate their crimes with others and personnel specifically trained in these specialized areas. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. CI [redacted] and had [redacted] to provide office supplies to the federal government. CI sold

products through GSA Advantage, an on-line catalog and preferred source of supply for federal and military customers. GSA supply contracts are referred to as schedule contracts, with each schedule representing a specific category of product or service. [redacted] holds a Schedule 75 contract under the office supply category.

8. CI [redacted] and CI was able to list [redacted] as a Veteran-Owned Small Business (VOSB) due to CI's veteran status. Pursuant to The Veterans Entrepreneurship and Small Business Development Act of 1999, government agencies are encouraged to buy from Veteran-Owned companies. These contracts are awarded solely to disadvantaged groups that qualify such as a VOSB. Due to CI's Veteran-Owned status, CI would have an advantage over commercial vendors for government sales. Pursuant to 48 CFR 52.219-1, VOSB companies must meet the following criteria: The VOSB must have a legitimate veteran who has 51% ownership and the VOSB must have a legitimate veteran who manages the daily business operations.

9. Pursuant to federal government contracting, the GSA maintains a central database that is used by federal agencies to display contractor details and specifics as well as eligibility to participate in federal programs such as the VOSB program. This database is referred to as the System for Award Management (SAM). The contractor must enter detailed information in the SAM about its organization and make annual certifications before it is allowed to bid on a federal contract.

10. Prior to the single database of SAM, GSA maintained two central databases that were referred to as the Central Contractor Registration (CCR) and Online Representations and Certifications Application. Although separate, these databases did share the same "user-input" data. The contractor was required to enter detailed information in the CCR about its organization

and make annual certifications in the ORCA before it was allowed to bid on a federal contract. The CCR server was located in Battlecreek, Michigan and the ORCA server was located in Sterling, Virginia.

11. In general, a contractor is required to have and be current in their SAM account to bid on a contract. The contractor first creates an account with a username and password, and then enters information into the system concerning the business. The contractor can log in, change, and update its SAM account at any time using the username and password. The contractor is required to annually review and certify its account in SAM. If a contractor's status changes during the period of the contract, the contractor is required to change its status in the SAM to reflect an accurate representation of its company. The SAM database maintains additions, modification and deletions that are made to a contractor's account and a "snap shot" of the Internet Protocol (IP) address of the location from where the additions, modifications and deletions were made.

B. Jurisdiction

12. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. See 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." Title 18, U.S.C., § 2711(3)(A)(i). This application is being submitted under Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

C. Locations to be Searched

13. As a Special Agent of the General Services Administration, Office of Inspector General, I make this affidavit as part of a request for the authority to search the following locations and facilities:

A. An address identified as [redacted] is maintained by and hosted at premises controlled by GoDaddy.com, LLC, an Internet service provider and remote computing service that is headquartered at 14455 N. Hayden Rd. Suite 219 Scottsdale, AZ 85260.

B. User account [redacted] that is stored at premises owned, maintained, controlled, or operated by GoDaddy, an Internet, domain, and email service provider headquartered at 14455 N. Hayden Road, Suite 219, Scottsdale, AZ.

C. User account [redacted] that is stored at premises owned, maintained, controlled, or operated by GoDaddy, an Internet domain, and email service provider headquartered at 14455 N. Hayden Road, Suite 219, Scottsdale, AZ 85260.

D. User account [redacted] that is stored at premises owned, maintained, controlled, or operated by GoDaddy, an Internet domain, and email service provider headquartered at 14455 N. Hayden Road, Suite 219, Scottsdale, AZ 85260.

E. User account [redacted] that is stored at premises owned, maintained, controlled, or operated by GoDaddy, an Internet domain, and email service provider headquartered at 14455 N. Hayden Road, Suite 219, Scottsdale, AZ 85260.

As further described in this affidavit, I have probable cause to believe there is now concealed at these locations evidence, fruits and instrumentalities; and contraband concerning certain crimes; or things otherwise criminally possessed, or which is designed or intended for use or which have been used as the means of committing criminal offenses to include: Title 18, United States Code § 287 (false, fictitious or fraudulent claims), Title 18, United States Code §

1001 (false statements), Title 18, United States Code § 371 (Conspiracy to commit offense or to defraud the United States), and/or title 18, United States Code § 1341 (mail fraud). I request authority to search these locations and facilities for the items described in Attachment A.

D. Background on remote computing services and the Internet

14. From my consultations with personnel familiar with stored electronic communications, and my own training, experience and knowledge, I am aware that:

a. The Internet is in part a computer communications network using interstate and foreign telephone and communication lines to transmit data streams, including data streams used to provide a means of communication from one computer to another and used to store, transfer and receive data and image files.

b. An "Internet Provider" (IP) address is a unique series of numbers, separated by a period, that identifies each computer using, or connected to, the Internet over a network. An IP address permits a computer (or other digital device) to communicate with other devices via the Internet. The IP addresses aid in identifying the location of digital devices that are connected to the Internet so that they can be differentiated from other devices. As a mailing address allows a sender to mail a letter, a remote computer uses an IP address to communicate with other computers.

c. An "Internet Service Provider" (ISP) is an entity that provides access to the Internet to its subscribers.

d. The term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

e. Domain names are used to identify one or more IP addresses. For example, the domain name "microsoft.com" represents about a dozen IP addresses. Domain names are used in Uniform Resource Locators (URL), and are used to specify addresses on the World Wide Web. A URL is the fundamental network identification for any resource connected to the web.

GoDaddy.com, LLC

15. GoDaddy.com, LLC (GoDaddy) is a business and company that operates as a remote computing service and is a provider of electronic communications services. GoDaddy is a publicly traded Internet domain registrar and web hosting company. It serves millions of customers globally. Customers and subscribers of GoDaddy are able to create accounts and then build and develop domains on the Internet to include web sites. GoDaddy also provides web hosting and online storage for information and data through GoDaddy's servers.

16. I have learned that GoDaddy provides a variety of on-line services to the public, including electronic mail (email). GoDaddy.com allows subscribers to obtain email accounts at the domain name of their choice, like the account listed in Attachment A. Subscribers obtain an account by registering with GoDaddy.com. During the registration process, GoDaddy.com asks subscribers to provide basic personal information. Therefore, the computers of GoDaddy.com are likely to contain stored electronic communications (including retrieved and un-retrieved) for all names and subscribers and information concerning subscribers and their use of GoDaddy services, such as account access information, transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

17. GoDaddy subscribers can also store information with the provider online. GoDaddy offers large scale storage and retention capabilities for files such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by GoDaddy. In my training and experience, evidence of who was using an account, including co-conspirators and victims, may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

18. In my training and experience, remote computing service providers such as GoDaddy (hereinafter also referred to as "providers") generally ask their subscribers to provide certain personal identifying information when registering for an email account.

19. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

20. In my training and experience, providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account.

21. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account, and the IP addresses associated with particular log-ins to the account. The IP logs contain addresses assigned to the user and the date stamp at the time the user accessed his or her profile. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account. Because the fraud being perpetrated is through the use of IP addresses and other electronic means, obtaining the information associated with the email and IP information is critical.

22. Messages, photos, audio videos, and other records that are stored on the providers' servers may not necessarily be located in the subscriber's home/work computer. The subscriber or user may store data on the providers' servers for which there is insufficient storage space in the subscriber's computer and/or which he/she does not wish to maintain in the computer at his/her residence or place of employment. A search of the files in the computer at the subscriber's residence or place of employment will not necessarily uncover the files that the subscriber has stored on the providers' servers. Therefore, the providers' servers are likely to contain all the material herein, including stored electronic communications and information concerning subscribers and their use of the providers' services, such as account access information, transaction information, and account application.

23. From my knowledge, training and experience, as well as consultation and discussions with other agents and personnel familiar with computer-related investigations, I know that it is common for individuals engaged in the criminal activities described herein to use websites, social networking sites, and other Internet-based applications to communicate with one another and facilitate their criminal activities. Such communications and the facilitation of

criminal activities include the use of these applications and electronic and stored data that would identify and describe: (a) other co-conspirators, aiders, and abettors who are participating in the illegal activities as well as the nature and scope of the illegal activities; (b) identify dates and locations where illegal activity has taken place or may take place in the future; (c) financial transactions and monetary transfers used to facilitate and continue criminal activities as well as the existence and location of records, bank accounts, and businesses pertaining to those activities; (d) sales and purchases of equipment, materials, and goods used to aid the co-conspirators in their endeavors as well as the location and use of assets accumulated; (e) travel, and locations where goods and materials are kept; and, (f) the existence of other communication facilities, including telephones, computers, email and other electronic accounts used by co-conspirators to communicate.

24. By their very nature, websites, networking accounts, and Internet-based applications described herein are kept and stored in computers and electronic-memory devices by the host companies, in addition to or in lieu of hard-copy versions of this data. Because such evidence is stored electronically, the data and evidence of the crimes described herein may be stored and be present for long periods of time.

25. In general, an email that is sent to a GoDaddy subscriber is stored in the subscriber's "mail box" on GoDaddy servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on GoDaddy servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on GoDaddy's servers for months or years thereafter.

PROBABLE CAUSE

26. I am currently assigned to an investigation of potential false statements involving [redacted] This investigation was initiated by the GSA, Office of Inspector General based on a suspicion that [redacted] and [redacted] were violating VOSB program regulations and falsifying data within GSA's SAM database.

27. Initial investigative efforts revealed that CI created a VOSB company named [redacted]

28. As stated earlier, two of the primary rules under the VOSB regulations state that the veteran has to control the day-to-day management and daily operations as well as be at least a 51% owner.

29. The following facts set forth there is probable cause to believe that the email addresses and accounts for [redacted] were used to assist and aid the subjects in committing VOSB fraud by violating the aforementioned program regulations.

30. In 2011, CI received a random email from [redacted] asking to purchase CI's home-based veteran-owned company, [redacted], along with the GSA contract [redacted] CI eventually met with [redacted] in Norco, California, at [redacted] also owned by [redacted] and ultimately sold [redacted] to [redacted] and his wife, [redacted] for $30,000. CI continued to work for [redacted] at a storefront location in [redacted] as a paid employee for approximately one year, until the storefront location closed in approximately 2013. CI later discovered that [redacted]

[redacted] continued to be listed as a veteran-owned business under CI's name, under the GSA contract. CI contacted [redacted] approximately every six months asking that CI's name be removed from the company.

31. On approximately November 12, 2015, [redacted] contacted CI and said that he had not been making any money, so he needed CI to stay on as the president of [redacted] for the purpose of using CI's veteran status. CI was told by [redacted] that someone named [redacted] would be contacting CI with details about staying on as President of [redacted] CI was contacted by [redacted] and was told that they just needed CI to sign an Operating Agreement, and agree to stay on as the President of [redacted] In return, they would pay CI $1,000 per year, and an additional $10,000 when the company was sold. CI told [redacted] that he needed time to think about it. On November 19, 2015, CI submitted a hotline complaint to the GSA-OIG, via email, pertaining to possible fraud regarding the use of CI's name and veteran status. After submitting the hotline complaint, CI started receiving emails from Thomas Dunlap using email address [redacted] regarding [redacted] and the Operating Agreement they wanted CI to sign. [redacted] and [redacted] were both cc'd in the email exchanges at their addresses [redacted] and [redacted] respectively. Additional emails were discovered during the investigation, including one for [redacted] at [redacted] one for [redacted] at [redacted] and one that was previously used by the CI, [redacted] when CI owned the company. The CI advised that he did not have access to the [redacted] emails after he sold the company to [redacted] in 2012.

32. The investigation revealed that the email address [redacted] continued to be used to sign the SAM representations and certifications in, 2014, 2015, 2016 and

2017. CI reiterated that he does not use that email address, nor did CI have access to it after he sold the company.

33. On January 21, 2016, [redacted] used email address [redacted] to electronically send the Operating Agreement to CI at [redacted] for review and signature; [redacted] were both cc'd on the email. During the investigation numerous emails were exchanged between CI, [redacted] at these same email addresses to discuss the Operating Agreement and to arrange future conference calls.

34. The Small Business Administration profile and GSA documentation for [redacted] shows that [redacted] uses a separate email address as the contact person for [redacted] which is listed as [redacted]

35. On January 25, 2016, the CI conducted a consensually monitored telephone call to [redacted] at [redacted] Dunlap conferenced in [redacted] to participate in the phone call. [redacted] stated that he is considered the CFO, [redacted] is considered the CEO, and [redacted] is considered the COO. [redacted] said that he and [redacted] take care of the legalese stuff, and [redacted] works more on the fulfillment end of it.

36. [redacted] stated that he and [redacted] were willing to pay CI $5,000 up front for signing the Operating Agreement which states that CI will be 51% owner of [redacted] and they will pay CI another $10,000 when they decide to sell the company. [redacted] stated that [redacted] is their International Development Company that is going to handle fulfillment for [redacted] and take care of paying all the bills. [redacted] said that [redacted] is a limited liability corporation so they have to follow various laws and have tax filings, and that it will protect the CI from some costs that come up and will double isolate CI from ever having to worry about being sued.

37. On February 1, 2016, CI conducted a consensually monitored telephone call to [redacted] who stated that he and [redacted] plan to sell the company in 2018, and they agreed to pay CI $1,000 to $2,000 per year if the company is not sold within five years. [redacted] agreed to send the $5,000 check to CI overnight upon signing the Operating Agreement. CI asked if he would have to do any work on behalf of [redacted] and [redacted] said, "No." Later in the conversation, [redacted] reiterated that CI didn't have to do anything regarding Allied Ink. This violates the VOSB standards, which requires the CI to control and manage daily business operations. [redacted] stated that [redacted] lives in [redacted] just across the lake from [redacted]

38. On February 3, 2016, I met with the CI and CI recalled that when Lin first asked CI to be listed as 51% owner of the company, CI told [redacted] that he should have a woman-owned business and put it in his wife's name. According to CI, [redacted] responded, "They asked me to, I told them no." CI said that it was at this point where CI realized [redacted] and [redacted] were controlling [redacted] and not [redacted]

39. CI contacted the GSA-OIG and advised that he had received the check for $5,000 payable from [redacted] via overnight FedEx. The return address showed: Origin ID: [redacted] This is the same location as other businesses owned and/or managed by [redacted] CI deposited the check into CI's checking account at the [redacted] The funds were later converted into a Cashier's Check and turned over to the GSA-OIG and placed into evidence on February 17, 2016.

40. On February 21, 2017, CI had a telephone conversation with [redacted] regarding the fact that [redacted] needed to re-incorporate [redacted] in Missouri; therefore, [redacted] requested

that CI provide him copies of [redacted] tax returns from 2011, 2012, 2013 and 2014. [redacted] talked to the State of Missouri, and they are allowing [redacted] to re-incorporate [redacted] in Missouri so long as [redacted] pays all the back taxes that are due. CI opined that [redacted] is running into trouble because they are out of compliance with their GSA contract by not being incorporated in Missouri. [redacted] advised that he cannot reconstruct the corporation in Missouri through [redacted] in California, so he plans to roll the business into an LLC, again under [redacted] in Missouri, instead. CI said that [redacted] told him again that he doesn't even need to do anything, and [redacted] told CI that he needs CI as "a body" in Missouri, and that they'd like to help CI make more money for being a "warm seat." This statement shows that [redacted] and [redacted] continue to use CI in a rent-a-vet scheme, which is a violation of VOSB regulations.

41. CI sold [redacted] in 2011 to [redacted] but CI recognized that his own name was never removed from the GSA contract. Later in 2015, CI was approached by [redacted] and eventually [redacted] and [redacted] and offered a straw deal to become 51% owner of [redacted] for the purpose of keeping CI's Veteran-Owned status.

42. On February 28, 2017, CI conducted a consensually monitored telephone call and CI asked about their GSA contracts; [redacted] responded that they already have a Schedule 75 contract and they are currently working on getting a Schedule 70 contract for computer hardware. It appears [redacted] may be trying to accumulate GSA schedule contracts.

43. On April 24, 2017, I received a copy of [redacted] SAM database records and an audit trail of entries made, changed and deleted from these records. As of today, [redacted] is listed as a VOSB in the SAM database, when in fact it is not operated by CI.

44. The SAM certifications list [redacted] as a VOSB and clearly certify that [redacted] is not less than 51% owned by a Veteran and that its management and daily business

operations are controlled by the Veteran. The user had to check a box to claim that [redacted] is a VOSB company.

45. A review of the 2014 and 2015 SAM audit trail showed that the IP addresses that were used to make the changes and/or certifications indicated they were made in [redacted] and for 2016 and 2017 the SAM was changed/certified in the vicinities of [redacted] This further indicates that the CI did not complete the annual SAM certifications and representations, which re-enforces the fact that CI is being used as a strawman.

46. As part of the SAM, users are required to complete the Representation and Certification section annually. In the certification, the user's name is auto-populated. For 2014 through 2017, the user fraudulently used the CI's name to complete this section, and when completing this section the user attested to the accuracy of the certification information. In addition, the certification provided that any misrepresentation may lead to criminal prosecution or civil liability.

47. There is probable cause to believe that [redacted] are fraudulently claiming VOSB status for [redacted] in order to provide them with an advantage they are not entitled to regarding sales of products to government customers. This deceptive activity subjects legitimate VOSB's to unlawful competition.

CONCLUSION

48. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on GoDaddy.com who will then compile the requested records at a time convenient to it; there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

49. I further request through the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Wendy J. Rowan
Special Agent
GSA-OIG

SUBSCRIBED and SWORN to before me this 3rd day of August, 2017

NANNETTE A. BAKER
United States Magistrate Judge
Eastern District of Missouri

ATTACHMENT A

I. TARGET SERVER and Execution of Warrant

This warrant is directed to premises owned, maintained, controlled, or operated by GoDaddy.com, LLC, or its subsidiaries, and applies to all content and other information within the Provider's possession, custody, or control associated with the computer server assigned the domain [redacted] (the "TARGET SERVER").

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the TARGET SERVER:

a. Server Content. All stored content information presently maintained on or otherwise associated with the TARGET SERVER;

b. Transactional Records. All transactional information concerning the TARGET SERVER, including IP address logs or other records of log-ins to the TARGET SERVER session dates and times, and durations;

c. Business records. All business records and customer information concerning the TARGET SERVER, including but not limited to: applications; account creation date and time; services utilized; length of service; full names, screen names, account names, telephone numbers,

email addresses, or other identification information associated with the customer; and methods of payment and detailed billing records.

d. Customer correspondence. All correspondence with the subscriber or other individuals associated with the TARGET SERVER, including complaints, inquiries, or other contacts with support services and records of actions taken.

e. Preserved records. Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of Title 18, U.S.C., Sections 287 – false, fictitious or fraudulent claims; 1001- false statements; 371 – conspiracy to commit offense or to defraud the United States; and 1341 – mail fraud, including any evidence concerning the following:

a. The contents of the domain account and user identification to include all subscriber, contact and personal identifying information, including: full name, user identification number, birth date, gender, contact email addresses, passwords, security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers and identifying information of individuals and technical infrastructure (e.g., servers and computers);

b. Information reflecting the identities of victims of the Subject Offenses;

c. Log files reflecting electronic events that occurred on the TARGET SERVER, including, but not limited to, remote access, file transfers, logon/logoff times, and system errors; all records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. Communications between and among the user(s) of the TARGET SERVER and any accomplices, confederates or aiders and abettors;

e. Other information that may assist law enforcement in determining the true identity and location of the user of the TARGET SERVER or his/her accomplices, confederates or aiders and abettors, including but not limited to: IP addresses, names, addresses, phone numbers, email accounts, social networking accounts, website registration accounts, credit card accounts, bank accounts, and payment records;

f. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

g. The types of service utilized; and

h. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH [redacted] THAT IS STORED AT PREMISES CONTROLLED BY GODADDY.COM, LLC	)	Case No. 4:17 MJ 5191 NAB

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Arizona
(identify the person or describe the property to be searched and give its location):

In the matter of the search of information associated with [redacted] that is stored at premises controlled by GoDaddy.com, LLC

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment A.

YOU ARE COMMANDED to execute this warrant on or before August 16, 2017 *(not to exceed 14 days)*
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nannette A. Baker, U.S. Magistrate Judge.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/3/17 at 16:01

Judge's signature

City and state: St. Louis, MO

Honorable Nannette A. Baker, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 4:17 MJ 5191 NAB	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

I. TARGET SERVER and Execution of Warrant

This warrant is directed to premises owned, maintained, controlled, or operated by GoDaddy.com, LLC, or its subsidiaries, and applies to all content and other information within the Provider's possession, custody, or control associated with the computer server assigned the domain [redacted] (the "TARGET SERVER").

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the TARGET SERVER:

a. Server Content. All stored content information presently maintained on or otherwise associated with the TARGET SERVER;

b. Transactional Records. All transactional information concerning the TARGET SERVER, including IP address logs or other records of log-ins to the TARGET SERVER session dates and times, and durations;

c. Business records. All business records and customer information concerning the TARGET SERVER, including but not limited to: applications; account creation date and time; services utilized; length of service; full names, screen names, account names, telephone numbers,

email addresses, or other identification information associated with the customer; and methods of payment and detailed billing records.

d. Customer correspondence. All correspondence with the subscriber or other individuals associated with the TARGET SERVER, including complaints, inquiries, or other contacts with support services and records of actions taken.

e. Preserved records. Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of Title 18, U.S.C., Sections 287 – false, fictitious or fraudulent claims; 1001- false statements; 371 – conspiracy to commit offense or to defraud the United States; and 1341 – mail fraud, including any evidence concerning the following:

a. The contents of the domain account and user identification to include all subscriber, contact and personal identifying information, including: full name, user identification number, birth date, gender, contact email addresses, passwords, security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers and identifying information of individuals and technical infrastructure (e.g., servers and computers);

b. Information reflecting the identities of victims of the Subject Offenses;

c. Log files reflecting electronic events that occurred on the TARGET SERVER, including, but not limited to, remote access, file transfers, logon/logoff times, and system errors; all records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. Communications between and among the user(s) of the TARGET SERVER and any accomplices, confederates or aiders and abettors;

e. Other information that may assist law enforcement in determining the true identity and location of the user of the TARGET SERVER or his/her accomplices, confederates or aiders and abettors, including but not limited to: IP addresses, names, addresses, phone numbers, email accounts, social networking accounts, website registration accounts, credit card accounts, bank accounts, and payment records;

f. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

g. The types of service utilized; and

h. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH [redacted] THAT IS STORED AT PREMISES CONTROLLED BY GODADDY.COM, LLC	)	Case No. 4:17 MJ 5191 NAB

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Arizona
(identify the person or describe the property to be searched and give its location):

In the matter of the search of information associated with [redacted] that is stored at premises controlled by GoDaddy.com, LLC

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment A.

YOU ARE COMMANDED to execute this warrant on or before August 16, 2017 *(not to exceed 14 days)*
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nannette A. Baker, U.S. Magistrate Judge
(United States Magistrate Judge).

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/3/17 at 16:01

Judge's signature

City and state: St. Louis, MO

Honorable Nannette A. Baker, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
4:17 MJ 5191 NAB	8/7/2017 11:09 AM	FAXED to (480) 624-2546 AS PER EMAIL INSTRUCTIONS from Compliance MANAGER.

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

ON October 18, 2017, Special Agent Wendy Rowan, GSA-OIG RECEIVED A letter from GoDaddy that they do not HAVE "A Computer SERVER ASSIGNED to the domain [redacted] Therefore, they do not HAVE ANY INFORMATION RESPONSIVE to the Search WARRANT.

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 10/24/2017

Wendy Jo Rowan
Executing officer's signature

Wendy Jo Rowan, Criminal Investigator
Printed name and title

ATTACHMENT A

I. TARGET SERVER and Execution of Warrant

This warrant is directed to premises owned, maintained, controlled, or operated by GoDaddy.com, LLC, or its subsidiaries, and applies to all content and other information within the Provider's possession, custody, or control associated with the computer server assigned the domain [redacted] (the "TARGET SERVER").

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the TARGET SERVER:

a. Server Content. All stored content information presently maintained on or otherwise associated with the TARGET SERVER;

b. Transactional Records. All transactional information concerning the TARGET SERVER, including IP address logs or other records of log-ins to the TARGET SERVER session dates and times, and durations;

c. Business records. All business records and customer information concerning the TARGET SERVER, including but not limited to: applications; account creation date and time; services utilized; length of service; full names, screen names, account names, telephone numbers,

email addresses, or other identification information associated with the customer; and methods of payment and detailed billing records.

d. Customer correspondence. All correspondence with the subscriber or other individuals associated with the TARGET SERVER, including complaints, inquiries, or other contacts with support services and records of actions taken.

e. Preserved records. Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of Title 18, U.S.C., Sections 287 – false, fictitious or fraudulent claims; 1001- false statements; 371 – conspiracy to commit offense or to defraud the United States; and 1341 – mail fraud, including any evidence concerning the following:

a. The contents of the domain account and user identification to include all subscriber, contact and personal identifying information, including: full name, user identification number, birth date, gender, contact email addresses, passwords, security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers and identifying information of individuals and technical infrastructure (e.g., servers and computers);

b. Information reflecting the identities of victims of the Subject Offenses;

c. Log files reflecting electronic events that occurred on the TARGET SERVER, including, but not limited to, remote access, file transfers, logon/logoff times, and system errors; all records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. Communications between and among the user(s) of the TARGET SERVER and any accomplices, confederates or aiders and abettors;

e. Other information that may assist law enforcement in determining the true identity and location of the user of the TARGET SERVER or his/her accomplices, confederates or aiders and abettors, including but not limited to: IP addresses, names, addresses, phone numbers, email accounts, social networking accounts, website registration accounts, credit card accounts, bank accounts, and payment records;

f. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

g. The types of service utilized; and

h. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

IN RE: SEARCH WARRANT	)	Case No.
	)	**FILED UNDER SEAL**

ORDER

The United States has submitted an application pursuant to Title 18, U.S.C. Section 2705(b), requesting that the Court issue an Order directing GODADDY.COM, LLC, hereinafter referred to as "the electronic communication or remote computing service provider," not to notify any person, including the subscribers or customers of the account(s), of the existence of a search warrant until further order of this Court. The search warrant requests information related to the following account(s):

[redacted]

The United States intends to serve the search warrant for the identified account(s) pursuant to Title 18, U.S.C. Section 2703. The Court determines that there is reason to believe that notification of the existence of the search warrant will seriously jeopardize the investigation, including by giving the subjects an opportunity to: flee, destroy, and/or tamper with evidence; change patterns of behavior; or notify confederates. *See* Title 18, U.S.C. Section 2705(b)(2), (3), (5).

IT IS THEREFORE ORDERED, pursuant Title 18, U.S.C. Section 2705(b) that the Application, search warrant, and this Order be sealed and that the electronic communication or remote computing service provider shall not disclose the existence of the Application, search warrant, or this Order until further order of the Court, except that the electronic communication or

remote computing service provider may disclose the search warrant to an attorney for the electronic communications or remote computing service provider for the purpose of receiving legal advice.

IT IS FURTHER ORDERED, that the government will: (a) notify the Court when either an indictment in this underlying investigation has been returned and unsealed or the government finalizes or closes the criminal investigation; and, when appropriate, (b) move this Court for an Order that allows the electronic communication or remote computing service provider to notify others of the existence of the search warrant.

IT IS FURTHER ORDERED, pursuant to Title 18, U.S.C. 2705(b), that the Application, search warrant, and this Order be sealed until further Order of the Court.

DATED: This 3rd day of August, 2017.

HONORABLE NANNETTE A. BAKER
United States Magistrate Judge

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF: INFORMATION ASSOCIATED WITH [redacted] THAT IS STORED AT PREMISES CONTROLLED BY GODADDY.COM, LLC	)	No. 4:17 MJ 5191 NAB **FILED UNDER SEAL**

ORDER

On motion of the United States of America, IT IS HEREBY ORDERED that the search warrant and affidavit and this Order issued thereto continue to be sealed until February 3, 2018, except for the limited purposes of providing same to defendant's counsel pursuant to Rules 12 and 16 of the Federal Rules of Criminal Procedure.

This Order is based upon the sealed motion of the Government establishing that: (a) the government has a compelling interest in sealing the documents in question which outweighs the public's qualified First Amendment right of access to review those documents; and (b) no less restrictive alternative to sealing is appropriate or practical.

HONORABLE NANNETTE A. BAKER
UNITED STATES MAGISTRATE JUDGE

Dated: 8/3/17